Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. Sections 1320d – 1320d-8 (2003), and its implementing regulations, 45 C.F.R. Parts 160 and 164 ("HIPAA Privacy Rule"), is a federal law that was enacted in part, to establish a national floor for the protection of certain personal health information. HIPAA's health information disclosure rules apply to "covered entities", a term defined to only include a health plan, a health care clearinghouse, and a health care provider who transmits protected health information in electronic form in connection with a covered transaction.

HIPAA applies to covered entities of State and local governments, but does not apply to aspects of State government that do not meet the technical definition of a covered entity. Medicaid and the Child Health Plan Plus are specifically named as covered entities. State nursing homes, mental health institutes and regional treatment centers are covered health care providers. Employers and workers compensation are specifically excluded from HIPAA's definition of covered entities. The State employee group health plan, flexible spending account plan and CSEAP plans are also covered health plans under HIPAA. Whether a State agency is a covered entity is a complicated matter dependent upon the facts and circumstances. Check with the State agency or department to determine if the contracting State agency is a covered entity under HIPAA. Each State covered entity should have a designated privacy officer that can be found on their website and HIPAA Notice of Privacy Practices.

Not all confidential medical information is protected by the HIPAA Privacy Rule. The HIPAA Privacy Rule only restricts disclosure of protected health information ("PHI") which is defined as individually identifiable health information that is transmitted or received in any medium by a covered entity, excluding certain educational and employment records. 45 C.F.R. § 164.501. As a general rule, the HIPAA Privacy Rule forbids a covered entity from using or disclosing a patient's protected health information without written authorization from the patient, except for treatment, payment, and health care operations. 45 C.F.R. § 164.506(a). Certain public interest disclosures are also permitted under section 512 of the HIPAA Privacy Rule.

If a covered entity uses an outside entity to perform covered functions on its behalf, and that outside entity has access to protected health information, that outside entity is considered a "business associate" under HIPAA. Covered functions means those activities that make a covered entity perform as a health plan, health care provider or health care clearinghouse and include: actuarial services, legal services, claims processing, collection, billing, and case management. A health oversight agency, such as the State Medical Board and Division of Insurance, is not business associates under HIPAA. HIPAA requires that the covered entity obtain written assurances from its business associates that they will use and safeguard PHI in accordance with the HIPAA Privacy Rule. A Business Associate agreement or addendum to a contract, is

required between any State Covered Entity and its business associates. There are two important exceptions to the requirement for a HIPAA Business Associate agreement. No agreement is required between covered health care providers to exchange PHI for treatment. No agreement is required between a health plan and providers where the only relationship between the parties is that providers are billing the plan for payment. Hence, a HIPAA Business Associate agreement is not required between Medicaid and every health care provider that bills Medicaid. Other data use, trading partner or provider agreements may be required for the exchange of confidential medical information between Medicaid and providers.

Contracts in place prior to October 15, 2002 that are not renewed or modified prior to April 14, 2003 must have a HIPAA business associate agreement in place by the earlier of the contract renewal or amendment date, or April 14, 2004. Most State contracts were renewed effective July 1, 2003 and were amended to include a HIPAA business associate addendum in the July 1, 2003 renewals. New contracts between State covered entities and their business associates entered into on and after April 14, 2003 are required to have a HIPAA business associate addendum on the date of the contract.

Business associates are required to take certain precautions, adopt policies and procedures and implement safeguards for their use and handling of the covered entity's PHI. The requirements for a business associate are found in the HIPAA Privacy Rule at 45 C.F.R. 164.504(e). In addition, all HIPAA business associate agreements must comply with the State's contract and fiscal rules. Many private sector vendors and providers do not understand that the State of Colorado has requirements in addition to the HIPAA business associate agreement requirements. For example, the HIPAA Privacy Rule does not require that business associates have insurance or indemnify the covered entity, however, the State of Colorado Fiscal rules require that all vendors have insurance and indemnify the State. No changes are permitted to the State Model HIPAA business associate addendum.